Attacks on hashing algorithms

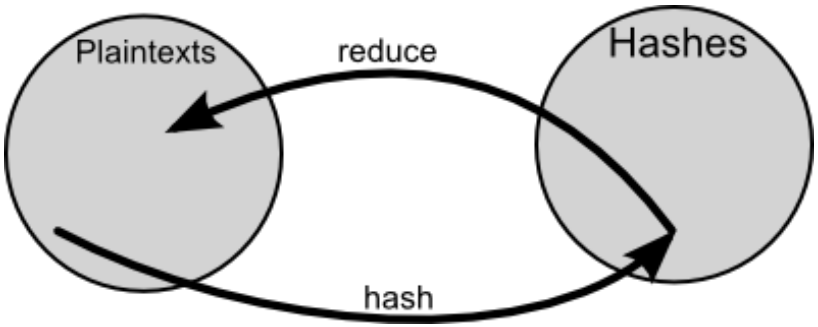
Hash precomputation

Precomputing hashes

- Space-time tradeoff
  - Save time in cracking the hashes (by precomputing them)
  - Pay the cost of storing them
- The naive and ugly way
  - `cat wordlist.txt | (while read WORD; do echo $WORD | md5sum | cut -c 1-32; done) > precomputed.txt`
    - *Slow: it executes using the CPU*
    - *Big output file*
      - *MD5 produces fingerprints of 32 characters (bytes)*
      - *Final size (in bytes): 32 x (n° of words)*

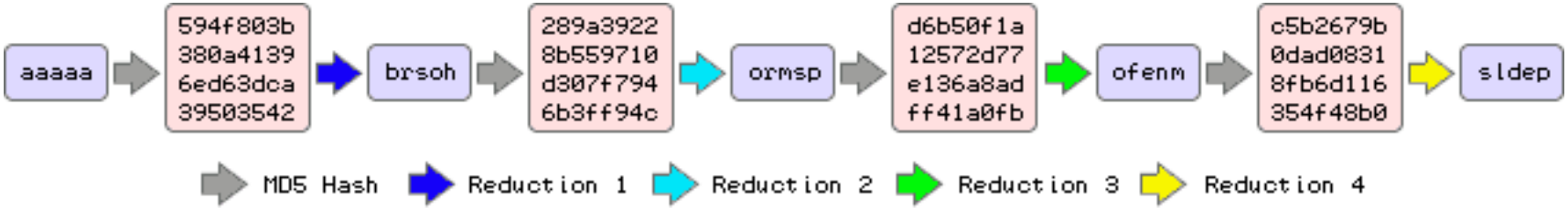
Rainbow tables

- Rainbow tables are more sophisticated (require less storage)
  - They use a **hash function** and a **reduction function** to store less data
- The reduction function maps values from the hash-value space to the pre-image space
  - i.e., a generic algorithm that takes a hash and transforms it to a password
  - The reduction function doesn't reverse the hash value, so it doesn't output the original plaintext (i.e. the password) — because this isn't possible — but instead outputs a completely new one

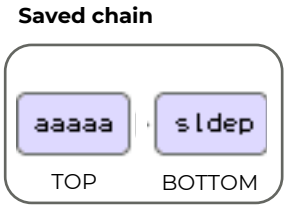


Rainbow tables: generation

- Multiple reduction functions are used
  - Each function corresponds to a “color” of the rainbow

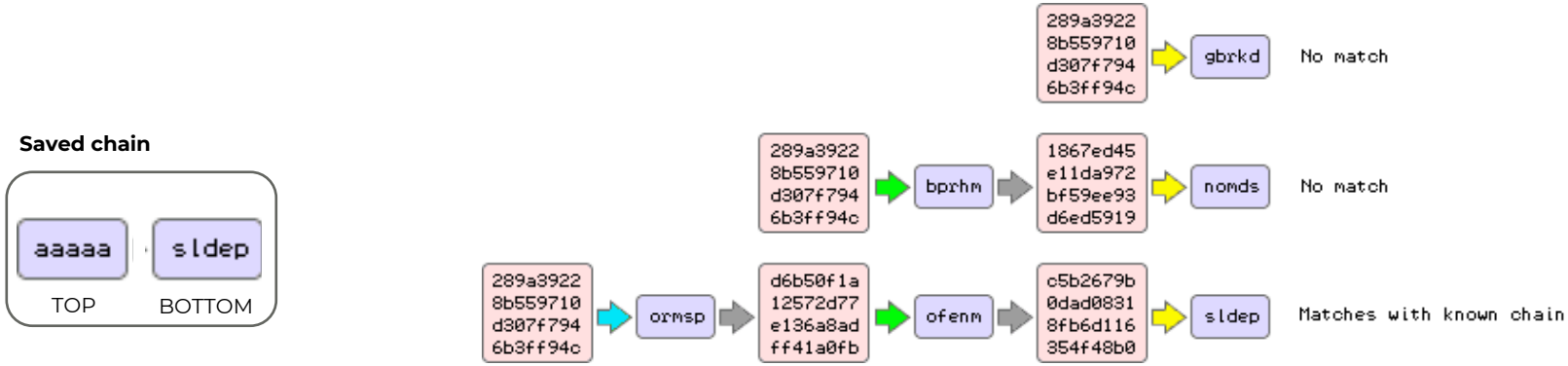


- Starting from a plaintext, the hash function and the reduction functions are applied in chain
  - Only the initial and final plaintexts are saved in the table
  - Lots of chains are generated



Rainbow tables: lookup

- Given a hash, iteratively apply the chain of functions (starting from the last)
- When the plaintext matches the bottom of one saved chain, pick the plaintext at the top and apply the whole chain until you find the input hash



DEMO

- Install **rainbowcrack**
  - `sudo apt install rainbowcrack`
- Generate a rainbow table
  - `sudo rtgen md5 loweralpha 1 7 0 1000 100000 0`
  - `sudo rtsort /usr/share/rainbowcrack`
- Crack a given hash
  - `rcrack  /usr/share/rainbowcrack -h (hash)`

Considerations

- Rainbow attacks are kind of "old fashioned"
  - Popular around the 2000s, especially for cracking Windows passwords
  - Only certain hashing algorithms are supported (MD5, SHA1, NTLM, …)
- This kind of attack may fail
  - Rainbow table must be sufficiently big to be useful (more chains, longer chains)
  - Generation takes a while, however rainbow tables can be conveniently shared

Buy Rainbow Tables

Detailed information of the rainbow tables is available in this page.

NTLM Rainbow Tables | MD5 Rainbow Tables | SHA1 Rainbow Tables | NTLM, MD5 and SHA1 Rainbow Tables

NTLM, MD5 and SHA1 Rainbow Tables (USD 2400)

Includes:

- Rainbow Tables

Table ID	Charset	Plaintext Length	Success Rate	Table Size
lm_ascii-32-65-123-4#1-7	All 95 characters on standard keyboard	1 to 14	99.9 %	27 GB
ntlm_ascii-32-95#1-7	All 95 characters on standard keyboard	1 to 7	99.9 %	52 GB
ntlm_ascii-32-95#1-8	All 95 characters on standard keyboard	1 to 8	96.8 %	460 GB
ntlm_mixalpha-numeric#1-8	a-z, A-Z, 0-9	1 to 8	99.9 %	127 GB
ntlm_mixalpha-numeric#1-9	a-z, A-Z, 0-9	1 to 9	96.8 %	690 GB